Approved For Release 2010/11/26 : CIA-RDP87T00623R000200070028-9

SECURITY POLICY ON INTELLIGENCE INFORMATION IN AUTOMATED SYSTEMS AND NETWORKS

(Effective 4 January 1983) [1]

Pursuant to the provisions of the Director of Central Intelligence Directive (DCID) on the Security Committee, policy is herewith established for the security of classified intelligence information (hereafter referred to as intelligence) [2] processed or stored in automated systems and networks.

1. Applicability

The controls and procedures in these provisions and the attached Computer Security Manual shall be applied by all Intelligence Community agencies. Intelligence Community agencies which release or provide intelligence to contractors, consultants or other government departments or agencies shall ensure beforehand that the intended recipients agree to follow these controls and provisions in their own processing or storing of intelligence in automated systems and networks.

Senior Officials of the Intelligence Community (SOICs) [3] shall ensure that the controls and procedures in these provisions and the attached manual are incorporated in regulations on this subject issued by Intelligence Community agencies.

The diversity and complexity of automated systems and networks in use by, or already designed for future placement in, the Community may not permit full compliance with these controls and procedures. Accordingly, SOICs are granted discretion on the application to their automated systems and networks of the exceptions stated in these provisions, consistent with the responsibility of SOICs for the protection of all intelligence in their custody.

2. Responsibilities

Each SOIC or his designee is responsible for ensuring compliance by his/her respective organization, and any other organization for which he/she has security responsibility, with these provisions and the attached Computer Security Manual. However, only an SOIC may accredit an automated system or network for operation in the Compartmented Mode.

3. Policy

SOICs shall establish and maintain within their agencies formal computer security programs to ensure that intelligence processed or stored by automated systems

---

[1] These provisions supersede those in DCID 1/16, effective 6 June 1982. They derive from and have the force of the DCID on the Security Committee, effective 15 July 1982.

[2] For purposes of this policy statement, classified intelligence information ("intelligence") means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources or methods, that has been classified pursuant to Executive Order 12356 (or successor Order). "Foreign intelligence" and "counterintelligence" have the meanings assigned them in Executive Order 12333. "Intelligence," as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982 (or successor manual).

[3] Senior Officials of the Intelligence Community (SOICs), for purposes of these provisions, are the heads of organizations within the Intelligence Community, as defined by Executive Order 12333, or their designated representatives for intelligence matters.

Approved For Release 2010/11/26 : CIA-RDP87T00623R000200070028-9

Approved For Release 2010/11/26 : CIA-RDP87T00623R000200070028-9

and networks is adequately protected. The minimum security requirements for the allowed modes of operation of automated systems and networks are contained in the attached Computer Security Manual. Additional computer security measures may be established if deemed appropriate. Automated systems or networks shared with foreign governments shall be addressed on a case-by-case basis by the SOIC(s) involved in consultation with the DCI or his designee for this purpose.

4. Exceptions

a. These provisions do not apply to automated systems or networks used exclusively for telecommunications services. Security policy on such services is provided by the National Communications Security Committee.

b. SOICs or their designees may temporarily exempt specific automated systems or networks under their jurisdiction from complete compliance with these provisions and the attached manual when compliance would significantly impair the execution of their missions. Chapter III of the attached manual governs when the system being exempted is part of an automated network as defined therein. An exemption may be granted only when the SOIC or his/her designee is assured that the other security measures in effect will adequately protect the intelligence being processed. The SOIC or his/her designee granting an exception shall strive for the earliest feasible attainment of complete compliance. No exception shall be granted which would allow personnel with less than a TOP SECRET clearance based on a background investigation to access an automated system or network which contains SCI.

c. Nothing in these provisions or the attached Computer Security Manual supersedes requirements under the Atomic Energy Act of 1954, as amended (Section II, Public Law 585), on the control, use, and dissemination of Restricted Data or Formerly Restricted Data, or requirements regarding Communications Security (COMSEC) related material as established by or under existing statutes, directives, or Presidential policy.

Attachment:
DCI Computer Security Manual

Approved For Release 2010/11/26 : CIA-RDP87T00623R000200070028-9